REMARKS

Reconsideration of the application is respectfully requested for the following reasons:

1. Rejection of Claims 1-4, 6, 11, and 13-17 Under 35 USC §102(b) in view of U.S. Patent No. 5,659,616 (Sudia)

This rejection is respectfully traversed on the grounds that the Sudia patent neither discloses nor suggests a **file signing tool**, as claimed, that is arranged to perform the functions of:

- receiving a file to be signed;
- accessing a smartcard, the smartcard performing all digital signing operations that require access to a private key;
- actually signing the file, as opposed to simply retrieving a file signed by the smartcard; and
- downloading the signed file to a terminal, all as recited in claim 1.

It is true that the system of Sudia discloses use of a smartcard to authenticate a transaction by providing a private key. However, the Applicant has not claimed to have invented the concept of signing files by using a private key, and authenticating the files by means of a certificate that includes the corresponding public key. Instead, the invention is directed to the use of **file signing tool** that enables use of private key encryption to authenticate files being downloaded to a terminal, such as terminal update programs.

In Sudia, the smartcard itself, *rather than a file signing tool*, signs the "transaction." There is no suggestion of a **file signing tool** of the type claimed. Use of the smartcard to sign "transactions" is appropriate in the context of Sudia, since transactions are files that contain limited information, such as amounts. In contrast, the claimed invention involves downloading of files of arbitrary size, such as operating program or database updates, to a transaction terminal rather than just signing of transactions. As a result, a separate tool is need to download the files to a terminal. In the context of the claimed invention, the smartcard is required to provide keys, but cannot perform the extensive calculations that might be necessary to sign a file of arbitrary size.

As a result, the Sudia patent does not disclose or suggest a **file signing tool** of the type claimed, which receives a file, causes a smartcard to perform operations that require access to a private key in order to sign the file, <u>use the results of the operations to sign the file</u>, and download the signed file to a terminal. Basically, the Sudia patent merely discloses the concept of protecting a private key using a smartcard. It does not disclose a file signing tool capable of signing "files" for download to a terminal, as claimed.

In item 4 on page 2 of the Official Action, the Examiner argues that the Sudia patent teaches "a file signing tool arranged to receive a file to be signed (Sudia, column 10, lines 2-5, private key), to access the smartcard (Sudia, column 9, lines 51-55), and to download signed files to the terminal (Sudia, column 9, lines 47-55, sign document and apply certificate), ..." However, col. 10, lines 2-7 of the Sudia patent reads as follows:

> *The particular sequence or order of required signatures may also be specified. Referring to FIG. 7, sending user A sends a transaction 702 signed 703 by his own smartcard 700 and, if user B's cosignature is required on the transaction 702, signed 704 by the smartcard of user B 701,*

This passage does <u>not</u> suggest a <u>file signing tool</u>, as claimed, for *accessing a smartcard.* Instead, the smartcard itself is used to sign a "transaction." Furthermore, col. 9, lines 47-55 reads as follows:

> *The user may be subject to transaction limits that control the value of transactions or other documents that the user may initiate. The user's signature will be valid only on transactions originated either up to a certain monetary limit or between two monetary value boundaries. Accordingly, as shown in FIG. 6, the sending user sends a transaction 601 signed 603 by the sender (actually by the user's smart card 600 containing his private key) and appends thereto an authorization certificate 604.*

This passage also does <u>not</u> suggest any sort of file signing tool, as claimed. Instead, it simply states that the smartcard signs a transaction. No separate file signing tool is disclosed, much less one that signs files and downloads them to a terminal. According to the claimed invention, the smartcard performs operations that require access to a private key stored thereon, but does not actually sign the files and download them to a terminal.

In summary, while it is true that Sudia teaches use of a smartcard to protect a private key, the claimed invention is not merely to protect a private key using a smartcard, but rather to provide a tool that permits a smartcard-protected private key to be used to authenticate files being downloaded to a terminal. Because the Sudia patent does not disclose or suggest all elements recited in the claims corresponding to original claims 1-4, 6, 11, and 13-17, withdrawal of the rejection under 35 USC §102(b) is respectfully requested.

2. Rejection of Claims 5 and 17 Under 35 USC §103(a) in view of U.S. Patent Nos. 5,659,616 (Sudia) and 6,092,202 (Veil)

This rejection is respectfully traversed on the grounds that the Veil patent, like the Sudia patent, neither discloses nor suggests a file signing tool, as claimed, that is arranged to perform the functions of receiving a file to be signed; signing the file by accessing a smartcard, and downloading the signed file to a terminal. Instead, the Veil patent suggests that even the private key itself may be read by a "security co-processor" to facilitate signing. **This is clearly contrary to the claimed invention**.

Reading of the private key stored on the smartcard is discussed in col. 11, lines 28-32 of the Veil patent. While reading if the private key is said to be optional, there is no attempt to limit operations that might compromise the key to the smartcard. The reason is that Veil is confident that use of a security co-processor will protect the key.

It is respectfully noted that the Veil patent discusses the possibility of having the smartcard performing all security functions, as in the Sudia patent, and dismisses the possibility on grounds of cost and practicality (col. 1, line 66 to col. 2, line 7). However, the solution proposed by the Veil patent is to add a security co-processor, rather than simply limiting key access operations to the smartcard while having a file signing tool perform signing operations that do not threaten key integrity. Thus, the Veil patent recognizes the problem addressed by the present invention, but teaches an alternative solution.

Furthermore, the Veil patent does not disclose a certificate that is installed on the terminal for use by the terminal in authenticating the signer certificate. According to item 11 on page 4 of the Official Action, this feature is disclosed in col. 13, lines 30-41 of the Veil patent. However, the cited passage actually refers to a cache of pre-verified certificates. In other words, the system of Veil stores pre-verified copies of the signer certificate, so that it only has to authenticate the signer's certificate one time, after which it merely checks to see if the received signer certificate is the same as a pre-verified one. This is not the same as authenticating a signer certificate using a *different* owner certificate. Accordingly, it is respectfully submitted that the Veil patent does not suggest modification of the system of Sudia to obtain the claimed invention, and withdrawal of the rejection of claims 5 and 17 under 35 USC §103(a) is respectfully requested.

3. Rejection of Claims 7 and 10 Under 35 USC §103(a) in view of U.S. Patent No. 5,659,616 (Sudia) and "*When A Password Is Not A Password*" (Weiss)

This rejection is respectfully traversed on the grounds that the Weiss article, like the Sudia patent, neither discloses nor suggests a file signing tool, as claimed, that is arranged to perform the functions of receiving a file to be signed; signing the file by accessing a smartcard, and downloading the signed file to a terminal. Instead, the Weiss article discusses the use of security tokens and challenge response scripts to *supplement* conventional single PINs or passwords. There is no suggestion in the Weiss publication of having a smartcard perform signing operations that might reveal a private key, while utilizing a file signing tool to perform the signing operation, nor is there is there a suggestion of using multiple PINs to protect access to the file signing tool and smartcard.

The challenge response arrangement if Weiss is clearly not the same as multiple PINs. PINs are numbers that are stored in the device for self-verification. In Weiss, a single PIN stored on the token is used to protect the token. The challenge-response protocol cited by the Examiner is not equivalent to the PIN, but rather is carried out by the controller of the terminal with which the token is to be used. As explained in the paragraph bridging pages 107-108 of the Weiss publication, entry of a <u>single</u> correct PIN provides access to a device. The challenge response routine does not even begin until after verification of the PIN, and involves encryption of the user's response ***by the token*** (*i.e.*, the smartcard), <u>access to the encryption device having been granted upon entry of the PIN</u>. **The challenge-response routine verifies the token, rather than protecting access to the token**. Thus, neither the password nor the challenge-response disclosed by Weiss can be considered equivalent to multiple smartcard-protecting PINs, as claimed.

Since the Weiss publication does not disclose the multiple PINs of claims 7 and 10, much less the file signing tool of claim 1, withdrawal of the rejection of claims 7 and 10 under 35 USC §103(a) is respectfully requested.

4. <u>Rejection of Claims 7 and 10 Under 35 USC §103(a) in view of U.S. Patent Nos. 5,659,616 (Sudia) and 5,7521,781 (Deo), and "*When A Password Is Not A Password*" (Weiss)</u>

This rejection is respectfully traversed on the grounds that the Deo patent, like the Weiss article and the Sudia patent, neither discloses nor suggests a file signing tool, as claimed, that is arranged to perform the functions of receiving a file to be signed; signing the file by accessing a smartcard, and downloading the signed file to a terminal. Furthermore, the Deo patent, like the Sudia patent and Weiss article, does not disclose the claimed requirement that multiple PINs be entered before access to the smartcard is granted.

Instead, the Deo patent discloses a system in which a smartcard is inserted into a terminal and exchanges certificates with a terminal to provide mutual authentication, with different PINs and certificates assigned to different applications. There is no suggestion of the terminal accessing the smartcard in order to sign a file for download to another terminal, and therefore the terminal of Deo cannot be considered to correspond to the claimed **file signing tool**. Furthermore, there is no suggestion of the claimed **multiple PINs** for accessing the smartcard. Instead, Deo discloses that different PINs are used to protect different applications on the smartcard. In the system of Deo, to access any particular application on the smartcard, **only a single PIN need be entered**. ***Requiring entry of different PINs to access different applications is not the same as requiring entry of multiple PINs before any access to the smartcard is granted.***

Withdrawal of the rejection of claims 7 and 10 under 35 USC §103(a) is accordingly respectfully requested.

Having thus overcome each of the rejections made in the Official Action, withdrawal of the rejections and expedited passage of the application to issue is requested.

Respectfully submitted,

BACON & THOMAS, PLLC

By: BENJAMIN E. URCIA
Registration No. 33,805

Date: March 3, 2005

BACON & THOMAS, PLLC
625 Slaters Lane, 4th Floor
Alexandria, Virginia 22314

Telephone: (703) 683-0500

NWB:S:\Producer\beu\Pending A...H\G\GOUGEON 893465\a01.wpd